ISAUnited
International Security Architects

Threat Intelligence Preparation-RP-212

Recommended Principle

Version 1-01.2024

www.isaunited.org

Forward

This guiding principle outlines the integration of 'Threat Intelligence Preparation' into your security architecture design. It refrains from prescribing detailed practices or instructions for every specific situation due to the intricate nature of industry and organizational technical architecture designs, encompassing infrastructure, complex networks, and associated components and systems.

Shall: As used in a standard, “shall” denotes a minimum requirement in order to conform to the standard.

Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the standard.

This guide should be used in conjunction with the practices described in the following ISAUnited standards and publications, when appropriate (use the latest revisions):

1. Security Design Operations Model
2. Defensible Architecture Design Methodology

Contents

Threat Intelligence Preparation-RP-212

Recommended Principle

Version 1-01.2024

Description

Threat Intelligence Preparation is a crucial component in the field of security architecture design, serving as a proactive and strategic approach to identifying and mitigating potential cyber threats. In the ever-evolving landscape of cybersecurity, organizations must be well-equipped to anticipate and counteract a diverse array of security risks. Threat Intelligence Preparation involves the systematic collection, analysis, and interpretation of information related to potential threats, enabling security professionals to better understand the capabilities, intentions, and tactics of malicious actors. By integrating threat intelligence into the architectural design, organizations can strengthen their defenses, enhance incident response capabilities, and ultimately fortify their security posture in the face of dynamic and sophisticated cyber threats. This proactive methodology empowers security teams to stay one step ahead in the ongoing battle against cyber adversaries, fostering a resilient and adaptive security architecture.

Scope

The scope outlines the comprehensive coverage of incorporating Threat Intelligence Preparation into the design of infrastructure, networks, and associated components and systems which assists in providing organizations with a framework to systematically integrate Threat Intelligence Preparation into their security architecture design. This principle emphasizes the critical reasons why security architects must have an in-depth knowledge of these principle elements.

Terms, Definitions, and Abbreviations

Architecture - Technical architecture refers to the structured framework that defines the design, organization, and integration of various technological elements within an IT system or enterprise. It encompasses hardware, software, networks, databases, and other components to create a cohesive and efficient structure that supports the organization's information technology strategy. Technical architecture provides a blueprint for the implementation, maintenance, and evolution of IT systems, ensuring alignment with business goals and optimal functionality.

Infrastructure - encompasses the foundational components, facilities, and systems necessary for the operation and functionality of an organization's information technology environment. This includes hardware, such as servers, data centers, networking equipment, and storage devices, as well as the associated software, middleware, and other supporting elements. Technical infrastructure provides the underlying framework for the deployment, management, and delivery of IT services, ensuring the reliability, scalability, and performance of an organization's technological capabilities.

Network - A technical network refers to the interconnected system of devices, communication pathways, and protocols that facilitate the exchange of data and information within a computer or telecommunications environment. It encompasses the hardware components like routers, switches, and cables, as well as the software protocols and configurations that enable seamless communication between computers and other devices. Technical networks are designed to support various functionalities such as data transmission, resource sharing, and access to services, forming the backbone of modern information technology infrastructures.

Components - any part of a system that, by itself, provides all or a portion of the total functionality required of a system. A component is recursively defined to be an individual unit, not useful to further subdivide, or a collection of components up to and including the entire system. A component may be software, hardware, etc.

Systems - a system is made up of one or more components, which may be linked (interact through the same processor) and or tightly coupled.

Threat Landscape - In the field of cyber threat intelligence, the term "threat landscape" refers to the comprehensive and dynamic overview of potential risks and hazards that an organization or system may encounter. The threat landscape encompasses a wide range of factors, including various types of cyber threats, vulnerabilities, and the potential impact of malicious activities on an organization's information technology infrastructure and network.

Security Culture

A favorable security culture is crucial for the security performance of the organization, regardless of its size or complexity. Security culture encompasses the shared attitudes, values, norms, and beliefs among employees and contractor personnel in the security department concerning risk and safety. In a positive security culture, collaboration among staff members is fostered, positive attitudes toward compliance are encouraged, a sense of responsibility for public safety and each other's well-being is instilled, and there is a fundamental belief in non-punitive reporting.

Given the numerous and intricate security activities within the organization, it is imperative to systematically manage security using an agreed framework and cultivate a positive security culture. While a positive security culture can exist independently, an effective SMS cannot thrive without it. Hence, security practitioners should actively strive to enhance and evaluate their security culture.

Sustaining a positive security culture demands ongoing diligence across the security department to address issues such as complacency, fear of reprisal, overconfidence, and normalization of deviance. Indicators of a positive security culture within the organization are provided below.

The organization:

- embraces security (personnel, public, and asset) as a core value,
- ensures everyone understands the organization's security mission, vision, and goals,
- fosters systematic consideration of risk, including what can go wrong,
- inspires, enables, and nurtures change, when necessary,
- allocates adequate resources to ensure individuals can accomplish their RP recommending the principle responsibilities,
- encourages employee engagement and ownership,
- fosters mutual trust at all levels, with open and honest communication,
- promotes a questioning and learning environment,
- reinforces positive behaviors and why they are important,
- encourages two-way conversations about learnings and commits to applying them throughout the organization, and
- encourages non-punitive reporting and ensures timely response to reported issues.

Adopting and implementing this recommended principle will strengthen the security culture of an organization. Leaders, managers, and employees acting to make safety performance and risk reduction decisions over time will improve architecture security as a value, thereby strengthening the security culture of an organization. With this RP, practitioners are provided an enhanced framework to manage and reduce risk and enable continual improvement in architecture security posture. The individual elements, when executed as deliberate, routine, and intentional processes result in improved communication and coordination, which yield a cohesive system and a stronger security culture.

Principle Elements

Applicability:
Target Audience: Specify the intended audience, including security professionals, architects, and stakeholders involved in the design and maintenance of organizational IT infrastructure and network.

Inclusions: Detail the specific components and systems within the organizational landscape to which Threat Intelligence Preparation applies, encompassing networks, servers, applications, and other relevant assets.

Framework Overview:
Conceptual Framework: Provide a high-level overview of the Threat Intelligence Preparation framework, elucidating its role in enhancing security resilience.

Integration Points: Identify key integration points within the security architecture where Threat Intelligence Preparation plays a pivotal role.

Key Components:
Threat Intelligence Sources: Enumerate and describe various sources of threat intelligence, including open-source feeds, industry reports, government alerts, and internal sources.

Data Collection Mechanisms: Define mechanisms for the systematic collection of threat intelligence data, ensuring a comprehensive and timely approach.

Analysis and Interpretation:
Analytical Processes: Detail the processes involved in analyzing and interpreting threat intelligence data, emphasizing the identification of relevant threats to the organization.

Intelligence Sharing: Highlight the importance of collaborative intelligence sharing within the organization and with external partners to strengthen collective security.

Implementation Guidelines:
Security Architecture Design: Provide guidelines for integrating Threat Intelligence Preparation into the design phase of security architecture, covering infrastructure, network design, and associated components.

Best Practices: Offer best practices for ongoing maintenance and adaptation of Threat Intelligence Preparation measures to address emerging threats.

Compliance and Governance:
Regulatory Compliance: Address the alignment of Threat Intelligence Preparation practices with relevant regulatory requirements.

Governance Framework: Define a governance structure for overseeing and maintaining Threat Intelligence Preparation initiatives.

Documentation and Reporting:
Record-Keeping: Specify requirements for documentation related to threat intelligence, ensuring a comprehensive record of activities.

Reporting Mechanisms: Outline reporting mechanisms for communicating threat intelligence findings to relevant stakeholders.

Review and Update:
Periodic Review: Establish a schedule for the periodic review and assessment of Threat Intelligence Preparation measures to ensure their continued effectiveness.

Continuous Improvement: Encourage a culture of continuous improvement by incorporating lessons learned from security incidents and emerging threat landscapes.

Informed Decision-Making:
Aligning Security Measures: By intimately understanding the infrastructure and network, security architects can align security measures with the specific needs and nuances of the organization. This alignment ensures that security is not an afterthought but an integral part of the organizational fabric, leading to more effective risk management.

Adaptability to Changes: Organizations undergo continuous changes in their infrastructure and network configurations. Security architects, equipped with ongoing knowledge, can adapt their security designs to accommodate these changes seamlessly. This adaptability is essential for maintaining an agile and resilient security architecture.

Responsibilities

Practitioner - The security practitioner shall establish and maintain the recommended principle and build a shared understanding of security culture. The security practitioner shall articulate expectations, including publishing a commitment to security, security responsibilities of personnel at all levels, policies, goals, and objectives. The security practitioner shall improve upon the recommended principle and measure its effectiveness and maturity in accordance with the requirements of this guidance document.

Management - Management shall actively promote, collaborate, communicate, sponsor, and provide support for this recommended principle.

General user - Users shall utilize and integrate this recommended principle into their operations and practices.

RACI - Responsibilities, accountabilities, and authorities in developing, implementing, and continuously improving the security shall be defined, documented, and communicated throughout the architecture practitioner's organization. Accountability for resource allocation shall be assigned to (an) management with appropriate authority.

Competence, Awareness, and Training

The security practitioner shall ensure that personnel whose responsibilities fall within the scope of the RP recommended principle have an appropriate level of competence in terms of education, training, knowledge, and experience. Where external resources, including contractors, are used to support the RP recommended principle, the security practitioner shall ensure that operating personnel have the requisite competence, skills, and experience.

The security practitioner shall define the need for and provide training to enable the development and implementation of the RP elements. Training shall include refresher training and raising awareness of where executing the safety assurance and continuous improvement sub-elements reveal opportunities to improve processes and procedures. Records of training shall be maintained.

The security practitioner shall establish a training schedule to ensure that personnel and contractors who have accountabilities, responsibilities, and authorities in executing the requirements of the RP are updated and aware of:

1.applicable elements of the RP recommended principle that affect their job requirements;
2. newly emerging or changing risks, problems in the execution of the RP, and opportunities to improve processes and procedures; and
3. potential consequences of failure to follow processes or procedures.

Summary

Implementing 'Threat Intelligence Preparation' recommended principles strengthens an organization's security culture and posture. The ongoing practice of caring about security strengthens the overall organization's belief in its value, acting as a unifying force to improve security posture. The execution of the elements depends on the actions of every individual and organizational unit at all levels of the organization. Each of the elements can be expected to contribute to different aspects of the security culture, and these combined aspects reflect the strength of the culture. The RP, with all its discrete elements, supports the culture, and the culture feeds back into the management system in a continuous process, yielding an increasingly mature organization.

References

1. NA

Revision	Date
Created Date	01-15-2024
Institute Date	01-22-2024
Published Date	01-22-2024

End of document.